SECURITY 2012

20. ročník konference o bezpečnosti v ICT

Zranitelnosti mobilních platforem

Lukáš Antal, Lukáš Bláha

AEC, spol. s.r.o.

Agenda

- Rooting/Jailbreaking
- Mobilní malware
- Možnosti infekce
- Činnost malware
- Jak se bránit
- Demonstrace zneužití zranitelnosti iOS

Rooting/Jailbreaking

- Získání práv uživatele root na daném zařízení

  = Získání plné kontroly nad daným OS
- Motivace uživatelů
  - Apple iOS
    - Instalace aplikací z necertifikikovaných repozitářů
    - Úprava uživatelského rozhraní OS
  - Android
    - Odstranění modifikací OS provedených výrobcem/operátorem
    - Instalace vlastních upravených ROM (CyanogenMod)

Mobilní malware I

- Malware
  - **Mal**icious soft**ware**
  - Souhrné označení škodlivého software
- Trojské koně
  - Instalace malware pod záminkou neškodné funkcionality
- Spyware
  - Krádež citlivých údajů
- Priviledge-escalation exploits
  - Zvýšení oprávnění zneužitím chyby v systému

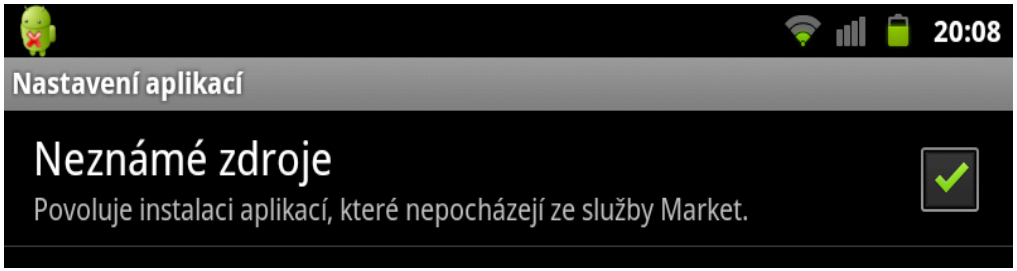
Reálný malware je kombinací výše uvedených kategorií

Mobilní malware II

- Reálná hrozba
- V roce 2011 nárůst o 273% [McAfee]
- Většina mobilního malware je cílena na platformu Android
- Proč?
- Distribuce aplikací
  - Apple iOS
    - App Store - centralizovaná autorita, každá aplikace prochází ručním prověřením
    - Jiné repozitáře - potřeba jailbreak
  - Android
    - Android market - volná pravidla pro přidávání aplikací, spoléhá na komunitu
    - Jiné repozitáře – pouze nastavení v telefonu

Možnosti nákazy I

- Instalace aplikací z nedůvěryhodného zdroje
  - Android – nastavení přímo v OS



  - iOS – nutný jailbreak

- V případě Androidu možnost infekce instalací aplikace z Marketu

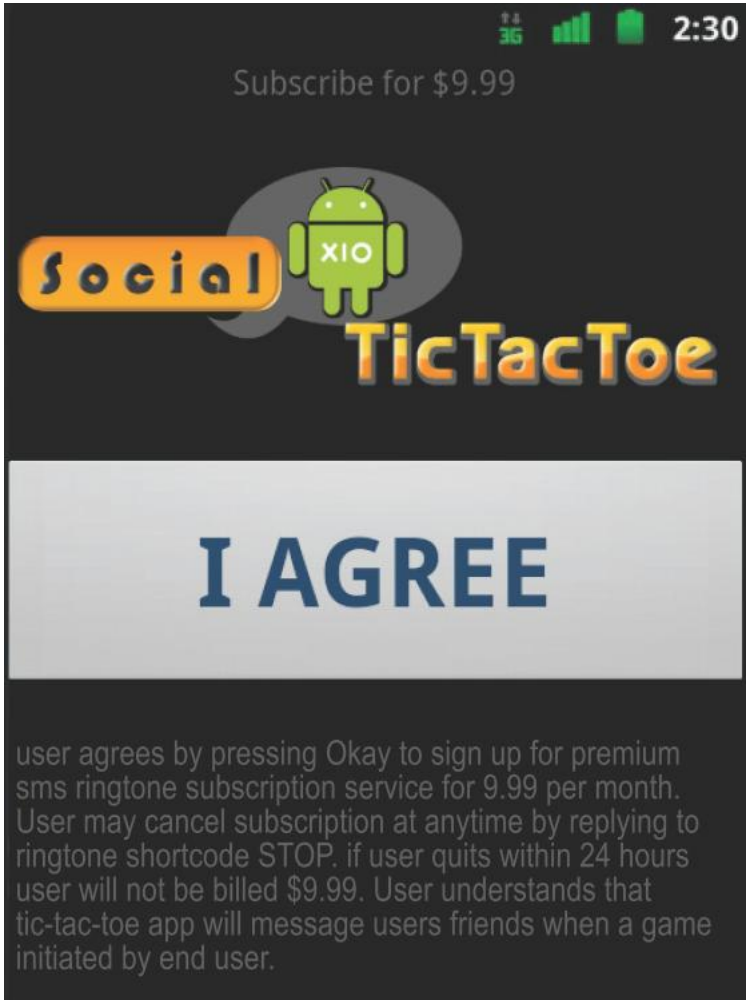
Možnosti nákazy II

- Malvertising
  - Malware advertising
- Phishing
  - Imitace webů (Android Market)
- Repackaging
  - Aplikace duplikována, přidán malware
- Falešný SW update
  - Aplikace bez nákazy, malware obsažen až v aktualizaci

Zdroj: www.mylookout.com

Možnosti nákazy III

- Nepozornost



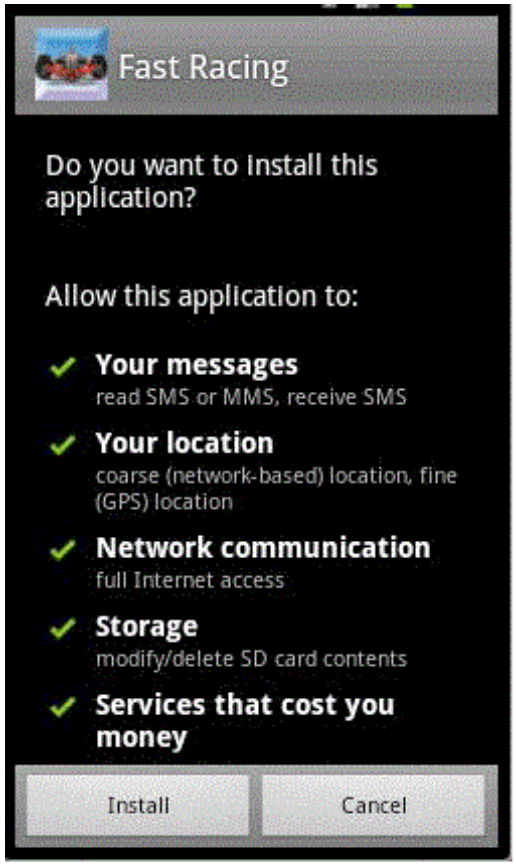
- User agrees by pressing Okay to sign up for premium sms ringtone subscribtion service for 9.99 per month …

Činnost malware

- Prémiové služby
  - Prémiové volání či SMS – vyšší tarifikace
- Odposlech hovorů a SMS
  - Hovory nahrávány a přeposílány útočníkovi
- Zapojení do botnetu
  - Dává útočníkovi možnost vzdálené kontroly
- Krádež citlivých dat
  - Fotografie, dokumenty, historie prohlížeče, uložená hesla
  - Krádež přihlašovacích údajů do IB (Zeus/ZitMo)
- Skrytá instalace dalších aplikací

Jak se bránit?

- Pravidelná aktualizace OS i SW
- Instalace aplikací z důvěryhodných zdrojů
- Kontrola práv aplikací
- Použití antiviru
- Použití šifrování
- Kontrola URL adres v prohlížeči
- Nastavení PINu a hesla
- Zamknutí telefonu při neaktivitě



Zdroj: www.trendmicro.com

Praktická demonstrace

Demonstrace zranitelnosti iOS zařízení

Získání přihlašovacích údajů

Co je potřeba k provedení útoku

- Fyzický přístup k zařízení
  - Za určitých specifických okolností není třeba!
- Jailbreak + Cydia

- Pro vzdálený přístup
  - OpenSSH, SSH klient, SCP klient, Keychain Dumper
- Na zařízení
  - Keychain Viewer

Jak se bránit

- Přístupový PIN / Passcode – složité získat přihlašovací údaje
- Neprovádět Jaibreak
- Hlídat si mobilní zařízení / nenechávat ho bez dozoru
- Remote Wipe - Find My iPhone

SECURITY 2012

20. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Lukáš Antal, Lukáš Bláha

AEC, spol. s r.o.